ICS 03.060
CCS A 11

Q/Bank of Qinhuangdao

秦皇岛银行股份有限公司企业标准

Q/Bank of Qinhuangdao 002—2023
代替 Q/Bank of Qinhuangdao 002-2022

网上银行

Internet Banking

2023-08-23 发布　　2023-08-23 实施

秦皇岛银行股份有限公司　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

本文件替代Q/Bank of Qinhuangdao 002-2022《网上银行》，与Q/Bank of Qinhuangdao 002-2022，相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“反电信网络诈骗治理安全”的内容（见4.1.2）；

b) 更改了“创新内容”的要求内容（见6.1.3，2022版的6.1.3）。。

本标准由秦皇岛银行股份有限公司提出并归口。

本标准起草部门：秦皇岛银行股份有限公司网络金融部、信息科技部。

本标准主要起草人：项海南、宣仰、吴頔。

本文件及其所代替文件的历次版本发布情况为：

——2019年首次发布为Q/130300 Bank of Qinhuangdao 001-2019，2020年第一次修订，2021年第二次修订，2022年第三次修订；

——本次为第四次修订。

引　言

根据《中华人民共和国标准化法》和《国家标准化发展纲要》，依据《市场监管总局等八部门关于实施企业标准“领跑者”制度的意见》（国市监标准[2018]84号），特制定秦皇岛银行网上银行服务标准，旨在规范网上银行系统建设、提升网上银行服务水平，促进网上银行业务规范、健康发展。

网上银行

1 范围

本标准规定了本行网上银行服务的规范，明确了本行网上银行服务的要求，确立了网上银行服务实施的保障机制。

本标准适用于本行通过互联网向客户提供的个人网上银行、个人手机银行、企业网上银行、企业手机银行等服务。

2 规范性引用文件

下列文件对本文件的应用是必不可少。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32315-2015 银行业客户服务中心基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

JR/T 0171-2020 个人金融信息保护技术规范

JR/T 0068—2020 网上银行系统信息安全通用规范

JR/T 0071—2020 金融行业网络安全等级保护实施指引

3 术语与定义

GB/T 32315-2015、GB/T 35273—2020、GB/T 39786—2021、JR/T 0171-2020、JR/T 0068—2020、JR/T 0071.1-2020界定的术语和定义适用于本文件。

3.1

网上银行 internet banking

商业银行等银行业金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其客户提供的网上金融服务。

3.2

个人网银 personal internet banking

商业银行等银行业金融机构面向个人用户提供的网上金融服务。

3.3

企业网银 corporate internet banking

商业银行等银行业金融机构面向企事业单位和其他组织提供的网上金融服务。

3.4

手机银行 mobile banking

商业银行等银行业金融机构通过移动通讯网络向客户提供账户查询、转账汇款、缴费充值、理财购买等金融交易服务。

3.5

数字证书 digital certificate

CA机构发行的一种电子文档，是一串能够表明网络用户身份信息的数字，提供了一种在计算机网络上验证网络用户身份的方式。

3.6

智能密码钥匙 cryptographic smart token

提供密码运算、密钥管理等密码服务的终端密码设备，一般使用USB、蓝牙、音频、SD等接口形态。

3.7

生物特征 biometric

人类生理上的或行为上的可测量特征，并由此可以可靠地区分某个人不同于其他人，以便识别登记者的身份，或者确认其所声称的已登记的身份。

4 服务安全性

4.1 基本安全要求

网上银行系统的安全技术、管理规范、业务运作安全、个人信息保护等均应符合GB/T 35273—2020《信息安全技术 个人信息安全规范》、GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》、JR/T 0068—2020《网上银行系统信息安全通用规范》、JR/T 0071—2020《金融行业网络安全等级保护实施指引》、JR/T 0171—2020《个人金融信息保护技术规范》等规定。

4.1.1 安全技术要求

4.1.1.1 客户端安全

应符合 JR/T 0068-2020 中 6.2.1 中客户端程序和客户端环境的要求。

4.1.1.2 网络通讯安全

4.1.1.2.1 通讯协议

应符合JR/T 0068-2020中6.2.3.1的基本要求，及以下增强要求：

a) 应使用加密算法和安全协议保护网上银行服务器与其他应用服务器之间所有连接，保证传输数据的机密性和完整性，协议版本应及时更新至安全稳版本，应采用 TLS1.1 及以上版本的 HTTPS 协议进行通信；
b) 应确保采用的安全协议不包含已知的公开漏洞。

4.1.1.2.2 安全认证

应符合JR/T 0068-2020中6.2.3.2的基本要求，及以下增强要求：

客户端程序和本地其他实体（指除支付软件自身外的其他软件及硬件）间的数据通信应采用安全的方式，确保通信数据不被监听和篡改。

4.1.1.2.3 通信链路

应符合JR/T 0068-2020中6.2.3.3的基本要求。

4.1.1.3 服务器端安全

4.1.1.3.1 等级保护要求

应符合JR/T 0068-2020中6.2.4.1的要求及JR/T 0071.1-2020、JR/T 0071.2-2020、JR/T 0071.3-2020、JR/T 0071.4-2020、JR/T 0071.5-2020、JR/T 0071.6-2020中有关安全技术要求，每年按照等级保护制度要求聘请专业测评机构开展等级保护安全测评。

4.1.1.3.2 安全通信网络

应符合JR/T 0068-2020中6.2.4.2的基本要求，及以下增强要求：

a) 使用带外管理的方式对网络设备进行管理，以保障数据网络和管理网络的物理信道分离；
b) 网络设备应支持 IPv6，针对 IPv6 的防护强度应不弱于针对 IPv4 的防护强度。

4.1.1.3.3 安全计算环境

应符合JR/T 0068-2020中6.2.4.3的基本要求，及以下增强要求：

a) 不应使用系统管理员账号进行业务操作；
b) 应保证操作系统和数据库的用户鉴别信息、重要业务数据所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
c) 支付敏感信息在应用层保持端到端加密，即保证数据在从源点到终点的过程中始终以密文形式存在；
d) 应支持数据库审计，并对 SQL 注入等攻击进行监控和报警；
e) 应对非法攻击行为进行监控，对其终端特征（例如，终端标识、软硬件特征等）、网络特征（例如，MAC、IP、WIFI 标识等）、用户特征（例如，账户标识、手机号等）、行为特征、物理位置等信息进行识别、标记和关联分析，并与风险监控系统实现联动，及时采取封禁等防护措施；
f) 应对恶意攻击行为进行分析，对恶意攻击事件按照网络安全相关要求及时进行上报处理；
g) 应探索采用运行时应用自我保护等技术手段，对恶意行为进行识别、阻断，多层次增强应用的安全防护能力。

4.1.1.3.4 虚拟化安全

应符合JR/T 0068-2020中6.2.4.4的基本要求，及以下增强要求：

a) 虚拟化环境加固应对虚拟机管理器进行完整性检查，确保虚拟机管理器加载的功能模块的完整性和真实性。
b) 虚拟机生命周期管理：
   1) 应严格保证虚拟机迁移过程中重要数据的机密性和完整性；
   2) 应防止虚拟机的跨安全域迁移。

4.1.1.3.5 传输安全

应符合JR/T 0068-2020中6.2.5.1的基本要求。

4.1.1.3.6 数据安全

应符合JR/T 0068-2020中6.2.5.2的基本要求。

4.1.2 反电信网络诈骗治理

4.1.2.1 账户准入

为核实客户身份真实性，完成开户尽职调查。上门核实时，要多方位、多角度了解客户相关信息，对于不熟知的客户，要通过多交谈获取更多客户信息，核实手段不限于现场查看客户是否有经营痕迹，向周围邻居打听经营情况等。经尽职调查确实存疑且客户无法提供相应佐证的，可根据实际情况酌情为客户开立账户。

4.1.2.2 异常账户管控处置

对人民银行、公安部门及总行下发的各类涉案账户清单要及时处置，保证“零延时”“零处罚”。对法定代表人失联、开户后无正常资金收付或存在小额试探性交易、联系方式异常、经营地址异常、对账异常的账户及存在久悬账户激活、存量账户变更法定代表人等存疑行为特征的账户要及时采取管控措施，有效化解和遏止账户管理风险。

4.1.2.3 客户分类分级

应通过账户分类分级管理，完成相应限额控制功能，从而有效防范账户涉赌涉诈、洗钱风险等。

4.1.2.4 风险检测

应对接风控返欺诈系统及反洗钱系统，在登录、设备绑定、智能转账、手机号转账等业务操作时，满足事中实时监测，对可疑交易监测机制中采取核实交易情况，如短信、人脸识别等验证手段，重新核验身份，确认异常交易给予中止。事后回溯排查，根据对接反洗钱系统以及账户分类分级系统等，对风险账户进行限额等控制，全流程监控网上银行系统风险。

4.2 服务连续在线可信性

4.2.1 服务时间

应满足7×24小时不间断运行。

4.2.2 运维应急人员配备

应配备7×24小时运维应急人员值班。

4.2.3 系统可用率

应采用集群、双中心双活等高可用技术保障服务连续运行，不应出现单点故障，系统可用率不低于99.99%。

4.2.4 数据丢失时间

应保证不发生数据丢失情况，数据丢失时间（RPO）0分钟。

4.2.5 系统恢复时间

在发生主数据中心故障时，网上银行系统恢复时间（RTO）应不超过30分钟。

4.2.6 可用性监控覆盖率

应达到100%，监控覆盖包括业务探针、硬件设备、网络、操作系统、数据库、主机进程、端口、应用性能等。

4.3 增强身份认证要求

4.3.1 增强身份认证技术要求

4.3.1.1 身份认证

身份认证信息应符合以下要求：

a) 登录密码复杂度应符合以下要求：
   1) 应区分大小写；
   2) 长度应不少于八位；
   3) 内容应至少包含字母、数字和特殊字符中的两种；
   4) 不应设为证件号、手机号等个人信息中的连续 6 位。
b) 交易密码复杂度应符合以下要求：
   1) 不应设为重复的单一数字，如 111111 等；
   2) 不应设为连 6 位数字，如 123456 等；
   3) 不应设为证件号、手机号等个人信息中的连续 6 位；
   4) 不应设为与登录密码相同的密码。
c) 应采用无感身份认证、智能风控、设备认证、传统身份认证等方式中的两种或两种以上维度对用户身份进行认证：
   1) 无感身份认证：对用户行为进行分析，判断异常行为，如更换常用 IP 登录、多次登录失败、频繁登录等，APP 给出相应提示，并且，通过风控系统判断是否存在风险；
   2) 智能风控系统：利用反欺诈识别，智能风控利用多维度、多特征的数据预测用户的欺诈意愿和倾向；配置多套风控规则，组合使用，针对客户的不同行为作出预测判断，给用户提供不同响应方式，以起到防暴力破解、防撞库、防盗用、防核身异常的目的；
   3) 设备认证：客户初次使用 APP 或者更换设备使用 APP 时必须进行设备绑定，并且要提供多重用户信息进行验证。针对设备切换频繁的用户，风控系统也进行了监控与响应。

4.3.1.2 密码安全

4.3.1.2.1 密码应用方案制定

密码应用方案制定应以保障资金安全为核心，在保证安全的同时，具有足够的易用性，降低使用门槛。应综合采用以下技术进行安全防范：

a) 信息防篡改：采用数字签名技术，对关键信息进行签名；
b) 信息加密:采用以国家标准或国家密码行业标准形式公开发布的密码算法对传输信息进行加密处理；
c) 用户方（发起方）确认：针对一笔交易，通过动态口令、支付密码、FIDO+、智能密码钥匙等技术确认用户身份；
d) 交易绑定：一笔交易使用一个无重复交易令牌，保障交易安全。

4.3.1.2.2 密码算法选择

密码算法选择应符合以下要求：

a) 客户端应采用以国家标准或国家密码行业标准形式公开发布的密码算法对资金有关交易或重要业务操作进行保护；
b) 密码算法、密钥长度及密钥管理方式应符合国家密码主管机构要求的国产商用密码算法提出要求；
c) 密钥在传输过程中应使用密码算法对密钥进行保护；
d) 随机生成的密钥应具有一定的随机性与不可预测性；
e) 密钥应加密存储，并确保密钥储存位置和形式的安全。

4.3.1.2.3 密码策略应用

密码策略应符合以下要求：
a) 客户端应采用 TLS1.1 及以上版本的 HTTPS 协议与服务器后台通讯；
b) 客户端应采用以国家标准或国家密码行业标准形式公开发布的密码算法对数据传输报文进行加密传输；
c) 服务器后台应采用加密机存储安全密钥，确保密钥储存位置和形式的安全。

4.3.1.2.4 密码安全性评估

密码安全性评估应符合以下要求：
a) 应符合密码应用安全性评估中的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置八项指标要求；
b) 应在信息系统规划阶段对密码应用方案进行评审或评估；
c) 应在信息系统建设完成后开展测评工作。

4.3.1.2.5 风险提示

网上银行系统运行环境进行安全评测，并根据安全评测情况对客户进行风险提示：
a) 应对运行环境的安全状况进行检测并向后台系统反馈，并将此作为风控策略的依据；
b) 应采取有效措施提升环境安全级别，针对不同的安全等级采取相应的风险控制措施；
c) 应在门户站点等渠道发布环境安全的提示；
d) 当发现环境存在重大安全缺陷或安全威胁时，应采取必要措施对用户进行警示或拒绝交易；
e) 如使用安全输入控件，该控件应具备监测自身是否正在被调试、截屏、录屏等情况的能力，并采取适当的风控措施。

4.3.2 增强身份认证机制要求

4.3.2.1 智能密码钥匙

应符合JR/T 0068-2020中6.2.2.1的基本要求，及以下增强要求：
智能密码钥匙应能够自动识别其是否与客户端连接，应具备在规定的时间与客户端连接而未进行任何操作时的语音提示、屏幕显示提醒等功能。

4.3.2.2 文件证书

应符合JR/T 0068-2020中6.2.2.2的基本要求，及以下增强要求：
在备份或恢复私钥成功后，金融机构应通过可靠的第二通信渠道向客户发送提示消息。

4.3.2.3 短信验证码

应符合JR/T 0068-2020中6.2.2.4的基本要求，及以下增强要求：

短信验证码时效性应不超过1分钟，超过有效时间应立即作废。

4.3.2.4 生物特征

应符合JR/T 0068-2020中6.2.2.5的基本要求。

4.3.2.5 其他机制

在本标准发布后新出现的专用安全机制，应根据自身特点参照上述分类的部分或全部要求，保证专用安全机制自身的可靠性以及其所保护信息的安全性。

4.4 风险控制能力

为保证客户交易安全，网上银行系统应对接智能风控系统，在登录、设备绑定、智能转账、手机号转账等业务操作时，应满足事前识别筛查、事中实时监测、事后回溯排查等要求，全流程监控网上银行系统风险。同时，应配备专门负责人员，及时处理异常交易及突发情况，有效的防范电信诈骗、账户盗用等网上银行渠道典型风险，主要内容包括：

a) 应加强服务开通环节控制，在网上银行系统申请受理中，柜台签约完成并确认客户签收认证工具后，方可为客户开通全部网上银行服务；
b) 应对接智能风控系统，通过对交易设备环境（设备型号、交易 IP、IP 解析城市、Wi-Fi 标示等）、用户行为、关联关系等维度综合评估计量交易风险，生成不同等级的风险标签，智能动态地针对不同等级、不同特征的风险交易采取差异化的安全控制措施；
c) 应组建专门风控运维队伍，制定事中风控运营体系与流程，开展实时交易监测、数据分析、人工核验、规则优化、模型建立与优化等工作，不断提升智能风控系统的风险识别能力；
d) 应按照国家监管部门规定开展反洗钱工作，认真执行反洗钱有关规定，切实履行反洗钱工作义务；
e) 应对客户进行风险意识宣传和安全教育培训，提升客户的安全、风险防范意识；
f) 解析出来的交易设备环境，均需记录保存数据，便于追溯；
g) 应严格遵守国家相关法律、法规、上级监管规定及我行网上银行各项规章制度进行运营管理和操作处理，保守商业秘密，不得擅自对外纰漏客户财务状况、各分支机构情况、账户信息和交易信息；
h) 应有针对网上银行各种安全事件的处理机制；
i) 应将重大安全隐患和运行事故及时报告至人民银行等金融主管部门。

5 服务体验

5.1 服务功能

5.1.1 个人客户

5.1.1.1 账户管理

a) 账户查询：
   1) 资产总览；
   2) 账户余额查询；
   3) 交易明细查询；

4) 账户开户行查询；
5) 交易回单查询。

b) 账户管理：
1) 账户别名维护；
2) 复制卡号；
3) 添加、删除账户；
4) 账户挂失、解除挂失；
5) 设置默认账户；
6) 主子账户绑定。

5.1.1.2 存款管理

a) 整存整取。
b) 通知存款：
1) 普通通知存款；
2) 通知利滚利。
c) 大额存单。
d) 零钱宝。
e) 月月富。

5.1.1.3 转账汇款

a) 智能转账。
b) 手机号转账。
c) 语音转帐。
d) 收款人管理。
e) 转账撤销。
f) 转账回单查询。

5.1.1.4 缴费充值

a) 缴费品种包括但不限于：
1) 暖气费；
2) 电费；
3) 燃气费；
4) 水费。
b) 充值品种包括但不限于：
1) 手机充值；
2) 流量充值。
c) 快速缴费。
d) 缴费记录查询。

5.1.1.5 投资理财

a) 理财产品服务：
1) 自营理财；
2) 代销理财。

b) 理财助手：
   1) 风险评估；
   2) 成交查询；
   3) 理财账单；
   4) 理财计算器；
   5) 利率查询。

5.1.1.6 公务卡服务

a) 公务卡还款：
   1) 给本人/他人还款；
   2) 自动还款签约；
   3) 账单分期；
   4) 现金分期；
   5) 消费分期；
   6) 分期查询。
b) 公务卡管理：
   1) 公务卡激活；
   2) 公务卡查询；
   3) 个人信息查询/修改；
   4) 挂失换卡；
   5) 查询/交易密码修改；
   6) 账单寄送设置。

5.1.1.7 安全中心

a) 安全认证方式管理：
   1) 登录方式设置；
   2) 登录密码管理。
b) 支付安全认证方式管理：
   1) 支付方式设置；
   2) 支付密码管理；
   3) 证书管理。
c) 限额管理：
   1) 转账限额管理；
   2) 小额免密支付；
   3) 面对面支付限额管理；
   4) 积分免密支付限额。
d) 权限管理：
   1) 资金归集协议管理；
   2) 三方支付协议管理。
e) 日志查询。
f) 解压密码查询。
g) 通知消息设置。

5.1.1.8 客户服务

a) 网点服务。
b) 人工客服。
c) 智能客服。
d) 功能搜索。
e) 个人信息维护。
f) 意见反馈。
g) 版本查询。
h) 信息保护政策。

5.1.2 单位客户

5.1.2.1 账户信息查询与对账

a) 账务总览。
b) 余额查询。
c) 交易明细查询。
d) 电子回单：
    1) 批量回单；
    2) 电子对账单。
e) 银企对账。

5.1.2.2 转账业务

a) 收款方管理。
b) 单笔转账。
c) 批量转账。
d) 代发业务。

5.1.2.3 票据业务

a) 出票管理。
b) 收票管理。
c) 票据查询。

5.1.2.4 投资理财

a) 定期存款。
b) 通知存款。
c) 大额存单。
d) 理财产品。

5.1.2.5 现金管理

a) 资金调拨。
b) 限额查询：
    1) 限额使用情况查询；
    2) 账户可用额度查询。

c) 现金池电子对账单。
d) 计价利息查询。

5.1.2.6 网银管理

a) 操作员管理。
b) 账户权限管理。
c) 业务流程设置。
d) 网银证书管理。
e) 消息中心。
f) 登录日志查询。
g) 转账限额设置。
h) 密码修改。

5.1.2.7 客户服务

a) 企业用户信息查询。
b) 在线客服。
c) 意见反馈。

5.2 服务性能

5.2.1 易用性

应符合以下要求：

a) 提供客户账户总览、产品筛选、功能搜索、产品推荐等服务功能，简易、高效地适应用户的使用需求和习惯；
b) 提供语音导航，方便客户使用；
c) 合理布局、输入简单，提供 OCR 图像识别自动录入介质、证件信息，粘贴板自动录入账号、证件号信息等功能；
d) 业务流程应符合客户普遍需求，减少操作步骤，使客户高效完成功能操作。

5.2.2 易学性

应符合以下要求：

a) 提供新用户使用指引；
b) 提供新功能使用指引；
c) 提供智能客服、人工客服方便客户咨询；
d) 提供一键反馈功能，并根据客户咨询反馈，设置重要问题解答。

5.2.3 舒适性

应符合以下要求：

a) 客户端应采用统一的 UI、VI 设计规范；
b) 版本应根据面向客群特点区别规划设计：
   1) 面向老年用户的“幸福生活版”App，字体、字号大于标准版；
   2) 面向视障用户的“关怀版”应减少图片、视频素材，扩大点击热区。
c) 文案应契合实际，使用日常、自然语言；

d) 图案应色彩搭配协调、图标风格统一；
e) 语音播报内容长度适中，语速、音量支持调整。

5.2.4 便捷性

应符合以下要求：
a) 支持功能搜索；
b) 设置常用功能区；
c) 支持客户定制页面内容；
d) 版本切换入口应清晰，保持客户访问版本；
e) 提供功能操作支持前进、返回，取消、确认，无断点；
f) 提供线上线下一体化服务，如网点查询、扫码付款等功能；
g) 提供用户日常生活缴费服务，并根据客户需求不断丰富。

5.2.5 易访问

应符合以下要求：
a) 支持从官方网站、主流应用商店下载客户端；
b) 客户端应支持记住用户名；
c) 移动客户端应支持指纹登录、手势登录和人脸登录等快捷登录方式；
d) 网点提供自助服务终端，方便客户登录、试用网上银行服务。

5.2.6 稳定性

应符合以下要求：
a) 系统应支持 7×24 小时服务；
b) 网上银行客户端、手机银行 App 运行稳定，不会出现页面错误、白屏等情况；
c) 闪退率≤0.05%；
d) 页面响应速度≤0.38 秒；
e) 超时时间设置≤10 秒。

5.3 客服代表行为规范

5.3.1 职业守则

客服代表职业守则主要包括：
a) 诚实守信：诚实不欺，恪守信用，品行端正，树立诚信理念，坚持信誉至上；
b) 遵纪守法：应以国家相关法律法规为行为准绳，严格遵守各项法律法规以及规章制度，认真学习法律知识，加强法律意识，自觉抵制违法违规行为；
c) 勤业尽职：应热爱自己的职业、岗位，精益求精、尽心尽职、奉公无私、兢兢业业，以高度的热情和责任心投入本职工作；
d) 专业胜任：应掌握相关业务知识，精通专业技能，根据社会发展、市场变化，在实践中不断学习新知识，钻研新技能，通过学习提高业务水平，适应工作发展的需要；
e) 严格守密：应具备保密意识，保护商业秘密与客户隐私。严格遵守保密法规，自觉履行保密责任，做到不失密、不泄密。不得以任何个人目的或原因，泄露商业秘密和侵犯客户隐私；

f） 宽容有礼：在工作中，会遇到各种各样的客户，在服务过程中，无论发生何种情况，都应时刻保持良好的观念和心态，保持宽以待人、谦虚诚实的态度，想客户之所想，急客户之所急，礼貌热情地为客户提供服务。

5.3.2 服务意识

应符合以下要求：

a） 应具有良好的心理素质和以客户为中心的服务理念，保持积极的服务态度；
b） 应主动倾听，注意力集中；不随意打断客户，保持与客户之间的良好互动。不应表现出不耐烦、推托之辞等现象；
c） 应主动服务，有较强的语言表达技巧和沟通能力，思路清晰，恰当引导客户，有效控制对话节奏，在客户对某些问题比较混淆时，能使用恰当语言总结性阐述客户问题，尽快切入正题，并能注意适当控制通话时间；
d） 应积极主动的为客户解答问题，主动提供相关信息或帮助，包括为客户介绍金融产品及服务；
e） 应指导客户使用电子渠道产品，引导客户使用办理相关业务的服务渠道、解决方法；
f） 应帮助客户在线办理金融业务；
g） 应了解客户需求，收集有益的客户建议，为改进服务和优化产品提供参考。

5.3.3 业务能力

应符合以下要求:

a） 应熟悉政策规定，熟练掌握本行业务制度和流程；
b） 应准确快速判断客户问题原因，了解客户实际需求；
c） 应根据客户类别和业务种类，及时解决客户问题；
d） 应熟练准确、回答完整，处理有效，正面回答，相关业务知识丰富，提示无遗漏并能提出适当建议，避免不必要持线；
e） 应对于超出解答能力范围的问题，与客户重复确认，主动记录客户问题，及时处理客户意见，妥善处理客户投诉，并在必要时跟进。

5.3.4 语言规范

应符合以下要求：

a） 应使用标准的开场白和结束语；
b） 应语速使用，匹配客户，和蔼、有微笑感，吐字清晰、流畅自然；
c） 应在客户等待或客户等待后对客户表示歉意；
d） 应使用“请、您、谢谢、对不起、请稍等”等礼貌用语；
e） 不应使用禁语，严禁与客户争吵，顶撞、辱骂客户，主动或借故挂断客户电话。

5.4 服务响应

应符合以下要求：

a） 电话客服平均响应时间≤15 秒；
b） 线上客服平均响应时间≤5 秒；
c） 提供 7×24 小时人工客服服务；
d） 电话客服接通率≥95%；
e） TCP 时间平均为 0.158 秒；
f） 平均加载时长≤0.395 秒。

6 创新及前瞻性

6.1 服务创新性

6.1.1 创新原则

网上银行服务创新应遵照《秦皇岛银行创新管理办法》，满足以下原则：

a) 依法合规原则：服务创新工作应在符合相关法律法规的前提下依法合规开展，符合监管机构要求及限制、符合本机构规章制度管理规定。
b) 风险可控原则：涉及风险进行全面且客观分析，风险管控应贯穿创新工作全流程。
c) 结果导向原则：创新工作以客户为中心，以市场为导向，提高效率、提升质量，追求综合利益最大化，提升整体核心竞争力，以更好的满足客户日益增长的需求，实现可持续发展。
d) 适当容错原则：应对创新出现的失误及风险，坚持适当容忍原则，对于事物或风险后沟及时进行报告、迅速纠正、弥补不良影响的应不予追究或从宽追究责任。

6.1.2 创新流程

创新过程应建立合理有效、流程清晰的创新流程管理体系，创新过程包括以下流程：

a) 需求发起：各部门、区域管理部、域外分行、支行均为创新发起部门，总行相关归口部门为需求收集与牵头部门。创新需求发起人应在综合考虑市场变化、目标客户需求的基础上结合我行现状，提出创新需求规划，采用逐级报送方式提交归口部门。
b) 创新立项：创新管理委员会办公室收集总行归口部门报送的创新需求方案，整理相关需求可行性文件，提前向涉及的业务、风险等部门征求意见，提交创先管理委员会进行审议，根据议定结果，协调、配合其相关立项、研发工作。
c) 创新研发：创新需求立项完成后，归口部门负责联合需求申请部门、配合部门进行创新项目开发。创新项目研发过程须依据创新流程节点，撰写书面报告。
d) 创新验收与测试：创新项目开发完成后，总行归口部门应负责组织进行创新成果测试与验收，出具验收报告并完成审批流程。
e) 创新评估与奖励：定期对创新项目进行评审，并对评审通过的优秀创新结果，根据项目创新性、价值性、效果性给予不同阶段、不同级别奖励。总行归口部门为创新后评估责任部门，负责在创新项目投产后，对完成情况、经济效益及价值进行评估及考核，并完成响应创新成果评估报告，将相应报告提交至创新管理委员会办公室。

6.1.3 创新内容

a) 针对不同客群，应提供差异化服务能力；
b) 应将生物识别、语音识别等能力应用于网上银行适老化及无障碍服务建设中，提高老年人及残障用户使用的便捷性，提升金融服务的获得感；
c) 适老化及无障碍设计应满足简洁性、易用性、稳定性和智能化要求：
   1) 简洁性：功能简洁、界面清晰、业务流程简明顺畅。客户端用户视图切换应支持双向切换，切换过程宜无需重启 APP；
   2) 易用性：操作简单便利、信息易读易理解（多感官通道、文本替代、语音读屏、统一交互），设计大字体、大图标、文字高对比度等功能特点的大字版版本，页面字体应可跟随 APP 字体或系统字体调整，保证老年人或视力较差人群也可以清晰阅读和使用；
   3) 稳定性：具备容错性及兼容性，客户端用户视图切换应支持双向切换，切换过程宜无需重启 APP；

4) 智能化：智能语音、智能搜索。

d) 适老化及无障碍设计应具有便利的引导流程，要求如下：
   1) 应制定功能变更使用指引说明，引导用户在功能发生变更后能及时熟悉、适应新功能，并指导用户使用新功能，帮助其掌握必要的技能；
   2) 系统在用户进行录入和选择操作时，及时校验用户录入和选择的信息，并提供相应提示，以提高用户输入的准确性。系统在任务失败后，为用户提示出现错误的原因并说明有效的解决方案。

e) 适老化及无障碍设计应采用创新性技术和应用措施：
   1) 支持读屏软件读屏；
   2) 标签按钮识读：对前端内部标签补全介绍，以便于读屏软件读取；
   3) 多媒体资源识读：将图片、利率展示等标签，补全成文本，保证视障人群可以清晰阅读。

f) 针对信贷客户，应提供 LPR 利率转换服务，实现可贷款业务查询及利率转换等操作；

g) 为助力乡村振兴，应针对村镇用户研发专属贷款产品，满足用户不同场景的贷款需求；

h) 根据网上银行用户特点，应为个人客户提供线上贷款服务，并规范展示贷款利率及贷款条件等信息，同时应支持线上申请、签约、提款、还款、查询等服务；

i) 根据经营地域特色，应为网上银行用户提供区域特色服务，例如：针对秦皇岛市冬季供暖用户提供热力缴费编号查询及缴费服务；

j) 应为客户提供非金融服务，丰富日常生活服务场景，提升居民缴费便捷性，例如：水费、电费、燃气费、通讯费及有线电视费缴费服务，满足村镇用户足不出可即可完成缴费，助力乡村振兴；

k) 针对用户投诉，应满足以下原则：
   1) 应在客户端首页醒目位置放置投诉客服电话，支持客户电话投诉和文本投诉两种方式，并安排专人定期查看留言情况；
   2) 应对于事实清楚、争议情况简单的投诉，处理时限一般不超过三个工作日；情况复杂或有特殊原因的，可延长至十五个工作日；情况特别复杂或有其他特殊原因无法在规定时限内完成的，应以电话等方式告知客户延长的理由和期限，并将延长时间和最后处理期限及时告知客户；
   3) 客户投诉处理过程中需外部机构进行鉴定、检测、评估等工作的，相关期间不计入投诉处理期限，但应即时告知投诉人；
   4) 经调查了解后，确属银行责任的，被投诉单位和当事人应主动向客户道歉，取得客户谅解，并对当事人进行批评教育和酌情处理，给客户造成经济损失的，应按有关政策规定给予赔偿。

6.2 技术前瞻性

a) 高可用架构：网上银行系统的生产、灾备中心支持应用级双活架构，数据库采用 Oracle ADG 模式进行数据同步。

b) 生物特征识别系统指标要求：
   1) 指纹特征识别：指纹特征识别系统错误拒绝率≤3%的情况下，错误接受率应≤0.001%；
   2) 人脸特征识别：人脸特征识别系统错误拒绝率≤5%的情况下，错误接受率应≤0.01%。

c) 生物特征识别系统技术创新与应用：
   1) 网上银行系统部分的手机银行采用快速安全身份认证系统 FIDO+作为登录、支付等重要业务的验证方式；
   2) FIDO+系统支持多种如“指纹认证”、“面部识别”等生物识别模式，提供安全、快捷、标准的身份验证方式；

3) FIDO+系统提供基于生物特征识别和 PKI 高强度密码认证的复合身份验证方式，采用 SM2、SM3、SM4 等国产密码算法，使用多级密钥体系，协议安全经过了形式化证明。

d) OCR 识别技术：网上银行系统部分的手机银行通过拍照或上传生成银行卡、身份证照片发送识别平台，平台进行算法处理生成最终识别出的证件信息的过程，通过 OCR 识别可大大提高业务操作效率以及检活繁琐的个人输入过程。

e) mPaaS 开发平台：mPaaS 开发平台具备消息推送、移动网管、发布服务、应用分析、数据同步，卡顿情况<2%，流量异常<0.1%，数据同步推送>50 条消息/S，冷启动<2S。

f) 灰度测试：生产环境分为灰度版本（生产白名单版本）和正式生产版本，两套系统共用基础数据。灰度版本作为对正式生产版本的提前版本，验证 APP 更新、新增功能、上线流程的正确性，为正式对外提供验证保障，降低对外应用的缺陷率。灰度版本，应该遵循上线更新流程，制定上线方案、应急预案、验证方案。

g) 设备指纹：检查设备运行环境，识别可疑上网设备，及时上报智能风控系统，智能动态地针对不同等级、不同特征的风险交易采取差异化的安全控制措施。

h) 客户端：统一网银登录入口，简化网银环境配置，增强客户信息安全，提升客户体验。

7 实施保障

7.1 组织保障

7.1.1 基本原则

网上银行业务由总行网络金融部统一管理，其他相关部门根据各部门职责参与网上银行业务管理。

7.1.2 部门职责

7.1.2.1 网络金融部

a) 负责牵头定制网上银行系统建设规划、业务管理办法等各项规章制度；

b) 负责汇总并提出网上银行业务整体需求，牵头业务需求部门进行验收测试并规划版本功能；

c) 负责跟踪调查、分析市场需求，制定并组织实施业务发展规划、市场推广计划；

d) 负责网上银行业务数据统计、分析及业务监控；

e) 负责与网上银行业务相关的第三方机构业务合作、业务外包管理等工作。

7.1.2.2 信息科技部

a) 负责网上银行系统软件服务、硬件设备采购；

b) 负责组织网上银行系统的功能开发、技术测试及系统投产工作；

c) 参与网上银行业务需求审定及测试案例评审；

d) 负责网上银行系统的日常技术运行维护，并建立系统监控和预警，实时监控系统运行，及时解决系统运行中出现的技术问题。

7.1.2.3 零售银行部

a) 负责收集客户、分支行关于网上银行零售业务的意见和建议，并提出本部门业务需求；

b) 参与本部门网上银行零售业务功能用户测试、验收测试和生产变更验证等工作；

c) 协助开展网上银行零售业务的营销推广和业务培训等工作；

d) 负责网上银行本部门相关业务客户咨询回复工作。

7.1.2.4 公司银行部

a) 负责收集客户、分支行等关于网上银行对公业务的意见和建议，并提出业务需求；
b) 参与网上银行对公业务功能用户测试、验收测试和生产变更验证等工作；
c) 协助开展网上银行对公业务的营销推广和业务培训等工作；
d) 参与制定网上银行对公业务建设规划、业务管理办法等各项规章制度等工作。

7.1.2.5 运营管理部

a) 按照本行凭证管理要求，负责智能密码钥匙等凭证进行入库、保管和调拨发放等工作；
b) 负责网上银行业务账务处理、资金清算结算、差错处理等工作；
c) 负责网上银行业务柜面功能菜单维护。

7.1.2.6 风险管理部

a) 参与审定网上银行业务风险控制策略；
b) 参与网上银行业务的风险评估。

7.1.2.7 区域管理部/分行

a) 负责收集所辖机构关于网上银行业务的意见和建议，并提出本机构网上银行业务需求；
b) 负责所辖机构网上银行业务管理，包括但不限于审批授权、合规检查、绩效考核、数据统计及业务运营分析等工作；
c) 负责对所辖机构网上银行业务营销指导和支持，组织业务培训、转培训；
d) 负责所辖机构网上银行业务风险管理，风险事件处置、上报等工作。

7.1.2.8 支行/网点

a) 负责负责办理具体网上银行注册、变更、注销等业务；
b) 负责拓展网上银行客户，制定本部门营销计划、实施推广活动；
c) 负责受理客户交易差错信息的查询，咨询解答，了解客户使用情况，及时向总行反馈客户需求；
d) 组织辖内单位定期开展网上银行业务检查、整改；
e) 配合总行做好对本单位网上银行业务的安全评估与内部审计；
f) 监督、检查和纠正本单位在网上银行业务开展过程中风险防范工作的执行情况；
g) 负责智能密码钥匙等凭证的领取、发放、保管和更换上交。

7.2 管理制度

7.2.1 产品研发

应符合《秦皇岛银行新技术、开源技术应用安全评估与准入规范V1.0》、《秦皇岛银行信息科技项目管理细则》、《秦皇岛银行信息科技应用软件开发规范_附件1_Java安全编程规范V1.2》、《秦皇岛银行信息系统开发管理细则》、《秦皇岛银行移动金融客户端标准》、《秦皇岛银行应用程序接口安全标准V1.0.0》、《秦皇岛银行源代码管理办法V1.0》、《信息科技应用软件Android 开发规范》、《信息科技应用软件IOS开发规范V1.1》、《秦皇岛银行信息系统安全开发测试管理制度》、《秦皇岛银行信息安全符合性管理制度》等管理制度的要求。

7.2.2 测试投产

应符合《秦皇岛银行信息系统测试管理细则》、《秦皇岛银行信息系统安全开发测试管理制度》、《秦皇岛银行变更发布管理制度》等管理制度的要求。

7.2.3 生产运营

应符合《秦皇岛银行信息科技资产管理细则》、《秦皇岛银行信息科技运维管理细则》、《秦皇岛银行信息科技外包管理细则》、《秦皇岛银行信息科技人员管理细则》、《秦皇岛银行数据安全管理细则》、《信息科技服务台管理规范》、《秦皇岛银行客户投诉处理管理办法》等管理制度的要求。

7.2.4 业务管理

应符合《秦皇岛银行个人数字银行业务管理办法（试行）》、《秦皇岛银行企业数字银行业务管理办法（试行）》等管理制度的要求。

7.2.5 应急响应

应符合《秦皇岛银行信息科技应急处置总体预案制度》、《秦皇岛银行软件开发项目应急预案》、《秦皇岛银行网络与信息安全应急预案》、《秦皇岛银行信息科技风险管理制度》、《秦皇岛银行信息科技信息系统应急预案》、《秦皇岛银行业务连续性管理办法》等管理制度的要求。

7.3 企业标准宣传及实施机制

7.3.1 宣传

a) 应在企业标准信息公共服务平台公开发布标准；
b) 应在自动化办公系统公开发布标准；
c) 积极参与企业标准的各类评选活动，对达到领先水平的标准通过电子屏、宣传折页、微信消息等形式，向客户宣传。

7.3.2 培训

a) 根据全行年度培训计划，将本标准纳入年度员工培训内容；
b) 根据网点晨夕会制度，将本标准纳入晨夕会学习范围。

7.3.3 实施

a) 应重点针对网上银行系统建设人员进行标准宣贯，严格按照标准要求进行功能开发；
b) 应建立网上银行服务监督机制，信息科技部负责对技术开发、运行维护等技术层面进行监督；
c) 网上银行业务主管部门对服务功能、管理办法等业务层面进行监督；
d) 客户服务主管部门负责对客服代表行为、服务响应等客户服务层面进行监督；
e) 应根据网上银行服务各主管部门监督情况，适时对标准进行更新修订。

参 考 文 献

[1] GB/T 32315-2015 银行业客户服务中心基本要求
[2] GB/T 35273—2020 信息安全技术 个人信息安全规范
[3] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[4] JR/T 0171-2020 个人金融信息保护技术规范
[5] JR/T 0068—2020 网上银行系统信息安全通用规范
[6] JR/T 0071—2020 金融行业网络安全等级保护实施指引